PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K

A2

(11) International Publication Number: **WO 98/50875**

(43) International Publication Date: 12 November 1998 (12.11.98)

(21) International Application Number: PCT/US98/09770

(22) International Filing Date: 8 May 1998 (08.05.98)

(30) Priority Data:
60/046,012 9 May 1997 (09.05.97) US

(71) Applicants: GTE GOVERNMENT SYSTEMS CORPORATION [US/US]; 1209 Orange Street, Wilmington, DE 19801 (US). GTE SERVICE CORPORATION [US/US]; 1209 Orange Street, Wilmington, DE 19801 (US).

(72) Inventors: DULUDE, Robert; 14 Lafayette Circle, Wellesley, MA 02181 (US). MUSGRAVE, Clyde; 3620 Fairfield Place, Frisco, TX 75035 (US).

(74) Agents: SUCHYTA, Leonard, Charles et al.; GTE Service Corporation, 600 Hidden Ridge HQE03G05, Irving, TX 75038 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: BIOMETRIC CERTIFICATES

(57) Abstract

Biometric identification is combined with digital certificates for electronic authentication as biometric certificates. The biometric certificates are managed through the use of a biometric certificate management system. Biometric certificates may be used in any electronic transaction requiring authentication of the participants. Biometric data is pre-stored in a biometric database of the biometric certificate management system by receiving data corresponding to physical characteristics of registered users through a biometric input device. Subsequent transactions to be conducted over a network have digital signatures generated from the physical characteristics of a current user and from the electronic transaction. The electronic transactions is authenticated by comparison of hash values in the digital signature with re-created hash values. The user is authenticated by comparison against the pre-stored biometric certificates of the physical characteristics of users in the biometric database.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

BIOMETRIC CERTIFICATES

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

This disclosure relates generally to the field of secure communications, and in particular to the issuance and management of certificates for authenticating messages.

2. DESCRIPTION OF RELATED ART

The use of computer networks and telecommunication systems for various transactions has markedly increased in recent years. Traditional transactions such as shopping, purchasing, banking, and investment services have experienced growth in new directions due to the application of computers and telecommunications.

While traditional transactions have heretofore been conducted typically on a person-to-person basis, many telecommunication-based transactions are conducted remotely and sight-unseen; i.e. the participants in telecommunication-based transactions may never meet.

With such telecommunication-based transactions, there is an increasing need to recognize and verify the authenticity of a remote user of electronic services, including such services involving consumers of all types of electronic transactions such as purchases over the Internet, home banking, electronic transfers of funds, and electronic brokerage services. Such electronic transactions may also involve users of remote

repositories of data, for example, to access classified records, medical records, billing records, and unclassified but sensitive data, such as company records. Other relevant areas requiring adequate or even absolute security include authentication of signers of electronic documents such as contracts. In general, any electronic service of value, provided over a local network or a public network, requires authentication of the requester in order to protect the value of the service. More valuable services typically require a greater degree of authentication.

Historically, access to electronic services has been provided through identification techniques such as account names and authentication techniques such as personal identification numbers (PINs) and passwords. Such authentication techniques have not proven to be very secure since PINs and passwords are often easily guessed, hard to remember, or subject to discovery by exhaustive automated searches. Recently, digital certificates have emerged as a leading candidate for authenticating electronic transactions.

Ideally, a digital certificate, such as those defined by the X.509 and ANSI X.9 standards, allows users or buyers and sellers to authenticate electronic documents and electronic transactions in a manner analogous to the authentication of documents by a Notary Public in person-to-person transactions. The combination of cryptographic techniques, including public key cryptography, and the use of digital certificates provides greater integrity, privacy and a degree of authentication for on-line electronic transactions which instills a greater level of confidence in the electronic services consumer.

For example, such authenticating certificates in the prior art may be generated by concatenating a message and a public key with a set 10 of data as shown in FIG. 1, which may be in a sequence and which may include a subject unique ID 12 corresponding to the subject; that is, the individual or entity such as a corporation, having the public key. As shown in FIG.

1, other fields in the set 10 of data may include a version number, a serial number for the certificate with respect to a sequence of generated certificates, the name of the issuer, a validity period to determine an expiration of validity of the certificate, a subject name identifying the user or individual sending the transaction, a issuer unique ID number, and other data extensions indicating privileges and attributes of the certificate, such as access privileges.

The subject unique ID 12 of the user may include M bits representing, for example, a social security number or a password associated with the user sending the transaction. Typically,

M ≈ 50 bits ≈ 6 bytes or less.

The authenticating certificate, being the concatenation of the set 10 of data with the public key and the transaction data, is then processed, for example, using a hash function such as a one-way hashing function, to generate a hashed value. The hashed value is then signed; that is, encrypted, using the private key of the user to generate a digital signature 14. The digital signature 14 is then appended to the authenticating certificate and the message, such as an electronic transaction, for transmission over, for example, a network.

The X.509 and ANSI X.9 standards described above incorporate a hash function to generate unique digital signatures 14 from a respective set 10 of data. Such one-way hashing functions enable the transaction data to be computationally infeasible to derive solely from the hash value.

While the use in the prior art of authenticating certificates incorporating digital certificates improves transactions employing electronic authentication, it still falls short of actually authenticating a human transactor, such as a consumer. Instead, such digital certificates in the prior art only authenticate the private cryptographic key used in the transaction or signature. Since private keys are physically

stored on computers and/or electronic storage devices, such private keys are not physically related to the entities associated with the private keys. For example, a private key is assigned to an entity, which may be a group of people, an organization such as a company, or even groups of organizations, and so private keys are not limited to actual human individuals.

Identification indica of individuals may be subdivided into three broad categories: indica based on the physical characteristics of the individual, that is, what the individual is; indicia based on one's knowledge, such as passwords known to the individual; and indicia based on assigned information, that is, what another individual has associated with the identified individual, or what the identified individual chooses with which to be associated. The first category having physical indicia relates to the biometric data of an individual, and includes characteristic features such as genetic composition, fingerprints, hand geometry, iris and retinal appearance, etc., which are unique to each individual, with known exceptions such as the identical genetic compositions of twins.

The second and third categories having known and/or assigned indicia includes information which the individual knows and/or is charged with memorizing and divulging for authentication, such as social security number, mother's maiden name, access codes such as long distance calling card numbers, and personal passwords. The second category also includes information and/or objects which the individual owns and/or is charged with carrying and divulging for authentication, such as driver's licenses and passports.

Private keys are assigned indicia. Accordingly, the lack of physical identification of a human transactor with a private key is a flaw in authentication techniques in the prior art using such private keys. Other authentication and security techniques in the prior art are similarly flawed, since many

authentication and security techniques rely on identification indicia of the second category.

Techniques are known in the art for authenticating an individual based on identification indica of the first category; that is, by physical characteristics. For example, U.S. Patent No. 4,641,349 to Flom et al. discloses a system for performing iris recognition. Typically, such physical characteristics identifying techniques require complicated computational operations for the capture and accurate classification of physical characteristics, since such physical characteristics are unique to each individual. Accordingly, the identification indicia for such physical characteristics generally requires a relatively large amount of memory to store and classify such identification indicia.

Heretofore, the relatively large computational demands of authentication techniques based on physical characteristics has prevented such authentication techniques from being implemented in electronic transactions.

SUMMARY OF THE INVENTION

It is recognized herein that biometric identification and classification in the authentication of electronic transactions provides for increased security and accuracy.

A biometric certification system and method are disclosed herein which implements an end-to-end security mechanism binding the biometric identification of consumers with digital certificates. The biometric certification system authenticates electronic transactions involving a user, and includes a biometric input device which responds to a set of physical characteristics of the user, and generates corresponding first biometric data related to the physical condition of the user.

Biometric data is pre-stored as biometric certificates in a biometric database of the biometric certificate management system by receiving data corresponding to physical characteristics of registered users through a biometric input

device. Subsequent transactions to be conducted over a network have transaction biometric data generated from the physical characteristics of a current user, which is then appended to the transaction first data, and which then authenticates the user by comparison against the pre-stored biometric data of the physical characteristics of users in the biometric database.

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the disclosed biometric certification system and method are readily apparent and are to be understood by referring to the following detailed description of the preferred embodiments of the present invention, taken in conjunction with the accompanying drawings, in which:

FIG. 1 illustrates an authenticating certificate in the prior art;

FIG. 2 illustrates a biometric certificate of the disclosed biometric certification system and method;

FIG. 3 illustrates a biometric certificate registration apparatus;

FIG. 4 illustrates an electronic transaction transmission section; and

FIG. 5 illustrates an electronic transaction reception and processing section.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring in specific detail to the drawings, with common reference numbers identifying similar or identical elements, steps, and features, as shown in FIG. 2 the present disclosure describes a biometric certification system and method for generating biometric certificates from a set 16 of data, including a subject unique ID 18 and biometric data 20. A digital signature 22 generated using data set 16 is then appended to the data set 16 to form the biometric certificate, as shown in FIG. 2.

The disclosed biometric certification system is shown in

FIGS. 3-5, having biometric registration section 24 shown in FIG. 3, a transmitting section 40 shown in FIG. 4, and a receiving section 42 shown in FIG. 5. The biometric registration section 24 processes user biometrics and associated inputs to generate biometric certificates which are unique to the user, and which are stored in a memory such as a biometric database and/or a smart card memory. Once such biometric certificates are stored, a first user may conduct biometrically-secured electronic transactions sent from the transaction transmission section 40 of FIG. 4 to the transaction reception section 42 of FIG. 5, at which the electronic transaction is authenticated and processed.

Referring to FIG. 3, the registration section 24 has a set of input devices, including a registration biometric input device 26 and a user data input device 28. The biometric input device 26 generates registration biometric data from the physical characteristics of the user, such as fingerprints, hand geometry, iris and retinal appearance, and speech patterns.

The registration biometric input device 26 may include visual cameras and/or other visual readers to input fingerprints, hand geometry, iris appearance, and retinal appearance. For example, companies such as IDENTIX, FUJITSU, and AUTHENTEC provide such equipment for reading fingerprints, while RECOGNITION SYSTEMS provides equipment to read hand geometry. EYE-DENTIFY is an example of a company which provides retinal imaging devices, while IRISCAN and SENSAR are examples of companies which provide iris imaging devices.

Alternatively, the registration biometric input device 26 may be adapted to receive audio characteristics of a user. For example, a microphone in conjunction with a speech digitizer may be used to receive and digitize speech. Such companies as BBN, T-NETIX, and ALPHA-TEL provide such equipment for receiving and digitizing speech to generate corresponding biometric data.

Biometric input devices known in the art may be used to receive other physical characteristics such as facial and body appearance via, for example, a camera, as well as the genetic composition of the user by means of genetic material gathering procedures, such as blood lancets.

The biometric certificate as shown in FIG. 2 may be generated by processing the registration biometric data from the registration biometric input device 26, processing the user input data such as a user ID from the user data input device 28, and processing the public key 30 of the user at a biometric certificate generator 32 of a registration authority 34. Such input data are processed with the private key 36 of a certifying authority to generate a digital biometric certificate 38 which is sent to the memory for storage and subsequent use to authenticate the first user and associated electronic transactions of the first user.

The registration biometric data 20 to be incorporated into the biometric certificate of FIG. 2 is obtained directly from the physical characteristics of the subject through the biometric input device 26. The subject unique ID 18 of the user may include M bits, in which typically M ≈ 50 bits ≈ 6 bytes or less, while the biometric data 20 typically includes much more data than the subject unique ID 18. Generally, the biometric data 20 has N bits in which N may be very large, such as about 500 bytes. In fact, the amount of the biometric data 20 is unlimited; for example, a fingerprint may be visually scanned to any resolution to obtain key fingerprint aspects which uniquely distinguish fingerprints, or alternatively to obtain data representing pixels of the entire fingerprint. Accordingly, the biometric data 20 may require large amounts of memory for storage such as 2 kB or even 4 MB. Accordingly, in the preferred embodiment, N is much greater than M.

Prior to use of the disclosed biometric certification system and method, the biometric database 66 is built using, for example, a registration process in which individuals are

required to provide proof of identity; that is, identification information such as a birth certificate, a driver's license, current bank account data, credit card account data, etc. to be provided to a registration authority. Once the registration authority is satisfied with such proof, the identification information is entered into the registration system 24 and biometric measurements are then taken concurrently using at least one biometric input device 26, as shown in FIG. 3.

Such stored biometric measurements form the pre-stored biometric data in the biometric database 66 which corresponds to the pre-registered individuals who have undergone the registration process described above. Accordingly, pre-registered individuals may be properly authenticated, while unregistered individuals are rejected, within the cross-over error rate.

The biometric certificates 38 are then sent to be stored in a memory, such as a biometric database or a memory of a smart card, as shown as the memory 66 in FIG. 5. The registration system 24 of FIG. 3 may be located at a central registration station associated with a network, such that the corresponding biometric certificates of a user may be directly and securely stored in the memory 66, such as a central biometric database of a network or an individual memory of a smart card of the user. Accordingly, the central biometric database as the memory 66 may serve a network of users conducting transactions, such as electronic commerce (E-commerce), over the Internet and other networks. Alternatively, a smart card of the first user having the memory 66 may pre-store the biometric certificates, such that kiosks and other devices such as terminals and automatic teller machines (ATMs) may access the memory 66 and obtain the secured biometric certificate of the first user.

Referring to FIGS. 4-5, to conduct an electronic transaction, the first user uses the transaction system 40 in FIG. 4. The first user uses a transaction biometric input

device 44 to generate transaction biometric data 46 as contemporaneous biometrics associate with the first user. The first user also generates transaction first data 50 through a transaction data input device 48. For example, the transaction first data 50 may include selections of products to be purchased over the Internet, or may include electronic funds transfers through an ATM. The transaction first data 50 also includes user ID data identifying the first user and associating the first user with the remainder of the transaction first data.

Both of the transaction biometric data 46 and the transaction first data 50 are sent over the network 60 unchanged and in the clear, or optionally encrypted by additional encryption techniques known in the art, to be received by the transaction reception section 42, as shown in FIG. 5.

In addition, at the transaction transmission section 40 of FIG. 4, both of the transaction biometric data 46 and the transaction first data 50 are processed, for example, using a first hash function 52, such as a one-way hashing function, to generate a first hashed value. RSA and SHA-1 are examples of public key cryptographic methods and one-way hashing which may be used for such encryption and hashing functions. The RSA method is described, for example, in U.S. Patent No. 4,405,829 to Rivest et al., which is incorporated herein by reference. The SHA-1 method is described, for example, in U.S. Patent No. 5,623,545 to Childs et al., which is incorporated herein by reference.

The first hashed value is then sent to a digital signature function 54, in which the hashed value is signed; that is, encrypted, using the private key 56 of the first user to generate a digital signature 58, incorporating the first hash value. The digital signature 58 is then sent to the network 60.

The set of data transmissions constituting the transaction

biometric data 46, the transaction first data 50, and the digital signature 58 may be sent as separate bitstreams and/or data packets, or otherwise may be sent together by appending the associated data sequences using a concatenator, such as an adder for bitwise adding of the data sequences. In addition, software may be used to append such data. The data 46, 50, and 58 may be sent to the network 60, which may include telephone networks, satellite communications, and/or the Internet.

Referring to FIG. 5, after receiving the electronic transaction from the network 60, the receiving section 42 sends the user ID data 62 from the transaction first data 50 to be sent to a biometric certificate extractor 54. The biometric certificate extractor 54 uses the user ID data 62 to access a corresponding biometric certificate stored in the memory 66, such as the biometric database or smart card memory. That is, if the first user had previously stored corresponding biometric certificates generated from biometric characteristics of the first user using the registration system 24 shown in FIG. 3, the biometric certificate of the first user may be indexed according to the user ID data, such as the social security number, of the first user.

The memory 66 may receive the user ID data 62, or otherwise may receive a command from the biometric certificate extractor 64 to retrieve any biometric certificate corresponding to the user ID data 62 of the first user. If none are available, the receiving section 42 may generate a rejection signal, for example, at the biometric certificate extractor 64, to indicate that no biometric certificate is available.

Accordingly, any user requesting authentication of an electronic transaction but failing to be registered; that is, to have a corresponding pre-stored biometric certificate stored in the memory 66, is not authenticated. The receiving section 42 may generate a corresponding message of non-authentication, and may also send such a message through the network 60 to the

transmitting section 40 to indicate no authenticity in the transaction.

Otherwise, if a biometric certificate is available for the first user having corresponding user ID data, the biometric certificate 68 is retrieved and sent to the biometric certificate extractor 64 to decrypt the biometric certificate 68 using the public key 70 of the certifying authority. Thus, the biometric certificate extractor 64 obtain the decrypted registration biometric data 72 and the decrypted user public key 74 associated with the first user.

The decrypted user public key 74 is then sent to a decryptor to decrypt the digital signature 58 sent over the network 60 from the transmitting section 24. The decryptor 76 then extracts the first hash value which was incorporated into the digital signature 58 by the first hash function 52.

The receiving section 24 authenticates the first hash value by attempting to recreate the first hash value using a second hash function 78 which is identical to the first hash function 52 of the transmitting section 24. The second hash function 78 receives the transaction biometric data 46 and the transaction first data 50 from the network 60, which were sent from the transmitting section 24 in the clear, or optionally encrypted by additional encryption techniques known in the art. The second hash function 78 thus generates a second hash value from the same input data applied to the first hash function 52.

The first and second hash values are then compared by a first classifier 80, such as a comparator or matching routines in software, for determining a match between the first and second hash values. A first validation signal 82 is generated to indicate whether or not both independently generated hash values match.

If both match, then the receiving section 42 thus determines that both of the transaction biometric data 46 and the transaction first data 50, in combination, are authentic and have not been modified during transmission over the network

60.

In addition, the receiving section 42 determines whether the electronic transaction is indeed from the indicated user corresponding to the transaction biometric data 46; that is, transaction biometric data 46 may not be authentic, or alternatively, the decrypted user public key 74 may be a public key 74 commonly shared by a specific group of people such as employees of a specific company.

Accordingly, the receiving section 42 compares the biometric data of the first user generated during the transaction, as the transaction biometric data 46, with the registration biometric data generated at an earlier date from the first user during a registration process using the registration system 24. The registration biometric data, which is decrypted by the biometric certificate extractor 64 to be the decrypted registration biometric data 72, is applied to a second classifier 84 to be compared to the transaction biometric data 46 which is sent over the network 60 in the clear, or optionally encrypted by additional encryption techniques known in the art.

The second classifier 84 may be a comparator, or alternatively a software routine or other hardware/software devices implementing data matching techniques, for comparing the biometric data to obtain a decision value. Alternatively, the second classifier 84 may be a trained neural network and/or a fuzzy logic classifier for classifying whether or not, within an error tolerance, the sets of biometric data 46, 72 were obtained from the same individual using biometric input devices. Such classification methods for authentication of images and data sequences using neural networks are described, for example, in U.S. Patent No. 5,619,620 to Eccles, which is incorporated herein by reference.

The second classifier 84 then generates a decision in the form of a second validation signal 86, which may be logic values corresponding to YES or NO, or TRUE or FALSE, indicating

verification of the authenticity of the user sending the electronic transaction. Alternatively, the authentication decision may be a numerical value, for example, corresponding to a percentage of confidence of authenticity. The second classifier 86 may include a predetermined threshold of, for example, 98% authenticity, to be exceeded in order to proceed with the processing of the electronic transaction.

The receiving section 42 shown in FIG. 5 may respond to the validation signals 82, 86 to process the transaction first data 50, such as an on-line purchase or an electronic funds transfer. Accordingly, transaction processing systems (not shown) may also be included in the receiving section 42. Alternatively, the receiving section 42 of FIG. 5 may be coupled to external transaction processing systems.

In another alternative embodiment, the receiving section may include an AND circuit 88 shown in FIG. 5, such as a logic AND gate or other logic mechanisms, for generating a final validation signal 90 from the validation signals 82, 86. Accordingly, if and only if both of the classifiers 80, 84 determine that the transaction biometric data 46 as well as the transaction first data 50 have been sufficiently securely transmitted over the network 60, then a final validation signal 90 reflecting the security of the overall transaction is generated.

Although the first classifier 80 is a perfect classifier; that is, only an exact match of the hash values generates an authentication, the second classifier 84 may generate percentages reflecting relative authenticity and/or scaled numerical values on an authenticity scale to reflect the error tolerance of the second classifier 84 and/or the cross-over error rates associated with biometrics. Accordingly, the application of fuzzy logic may be used to generate a crisp determination of the authenticity of the transaction biometric data 46 as the second validation signal 86.

Using biometric certificates, cross-over error rates for

identification and authentication may be below about 2.0%, and may even be also low as about 0.5%. The application of more advanced biometric input devices 26, 44 and classifiers 80, 84 known in the art may obtain substantially perfect authentication of any individual from the global population.

The disclosed biometric certification system and method may include electronic transactions using a network as described in commonly assigned U.S. Patent Application No. 08/770,824, filed December 20, 1996 and entitled "VIRTUAL CERTIFICATE AUTHORITY, which is incorporated herein by reference. Such a system can be adapted to include the use of biometric certificates as described herein for cryptographically binding the biometric data of a user with identification information to form such biometric certificates. The use of public key technology allows the transaction/signature authentication process to be done either centrally or remotely, depending upon the needs of the transaction.

While the disclosed biometric certification system and method is particularly shown and described herein with reference to the preferred embodiments, it is to be understood that various modifications in form and detail may be made therein without departing from the scope and spirit of the present invention. Accordingly, modifications, such as any examples suggested herein, but not limited thereto, are to be considered within the scope of the present invention.

CLAIMS

WHAT IS CLAIMED IS:

1. A biometric certification system for certifying an electronic transaction from a user, the electronic transaction including transaction biometric data, transaction first data, and a digital signature generated therefrom, the biometric certification system comprising:

a biometric certificate extractor, responsive to a biometric certificate corresponding to user identification (ID) data included in the transaction first data, for extracting registration biometric data and a user public key therefrom;

a decryptor, responsive to the registration biometric data and to the user public key, for retrieving a first hash value from the digital signature;

a hash function, responsive to the transaction biometric data and the transaction first data, for generating a second hash value therefrom; and

a first classifier for comparing the first hash value to the second hash value, and for generating a first validation signal to authenticate the transmission of the transaction first data and the transaction biometric data.

2. The biometric certification system of claim 1, wherein the biometric certificate is in the form of a sequence, including:

the registration biometric data;

user input data;

the public key of the user; and

the digital signature.

3. The biometric certification system of claim 2, wherein the portion of the bit sequence including the first biometric data is greater than about 500 bytes in length.

4. The biometric certification system of claim 1,

wherein the first classifier includes a processor for performing data matching procedures.

5. The biometric certification system of claim 1, further comprising:

a second classifier for comparing the registration biometric data and the transaction biometric data, and for generating a second validation signal to authenticate the user.

6. The biometric certification system of claim 1, wherein the second classifier is a neural network trained from a set of biometric data stored in the biometric database.

7. A biometric certification system for authenticating an electronic transaction involving a user, the electronic transaction including transaction biometric data, transaction first data, and a digital signature generated therefrom, comprising:

a transmitting section including:

a transaction biometric input device responsive to a set of physical characteristics of the user, the transaction biometric input device generates corresponding transaction biometric data related to the physical condition of the user;

a first hash function generator, responsive to transaction first data and the transaction biometric data, for generating a first hash value signal therefrom;

a digital signature generator which generates a digital signature from the hash value and a private key signal of the user; and

a receiving section operatively connected to the transmitting section through a network, the receiving section including:

a biometric certificate extractor, responsive to a biometric certificate corresponding to user identification

(ID) data included in the transaction first data, for extracting registration biometric data and a user public key therefrom;

a decryptor, responsive to the registration biometric data and to the user public key, for retrieving the first hash value from the digital signature;

a second hash function generator, responsive to the transaction biometric data and the transaction first data, for generating a second hash value therefrom; and

a first classifier for comparing the first hash value to the second hash value, and for generating a first validation signal to authenticate the transmission of the transaction first data and the transaction biometric data.

8. The biometric certification system of claim 7, wherein the transaction biometric input device is a visual reader which obtains hand geometry images of the user to generate corresponding biometric data.

9. The biometric certification system of claim 7, wherein the transaction biometric input device is a visual reader which obtains iris images of the user to generate corresponding biometric data.

10. The biometric certification system of claim 7, wherein the transaction biometric input device is a visual reader which obtains retinal images of the user to generate corresponding biometric data.

11. The biometric certification system of claim 7, wherein the transaction biometric input device is a visual reader which obtains facial images of the user to generate corresponding biometric data.

12. The biometric certification system of claim 7,

wherein the transaction biometric input device is a visual reader which obtains body images of the user to generate corresponding biometric data.

13. The biometric certification system of claim 7, wherein the transaction biometric input device includes:

a sound transducer that receives speech from the user; and

a speech digitizer which digitizes the received speech to generate corresponding biometric data.

14. The biometric certification system of claim 7, wherein the second classifier is a neural network trained from a set of biometric data stored in the biometric database.

15. The biometric certification system of claim 7, further comprising:

a logic circuit for generating a final validation signal from the first and second validation signals.

16. A method for authenticating an electronic transaction involving a first user, comprising the steps of:

registering a user, including the steps of:

receiving a registration set of physical characteristics of the user at a biometric input device;

generating registration biometric data corresponding to the registration set of physical characteristics;

generating a biometric certificate from the registration biometric data, user input data, the public key of the user, and a digital signature; and

storing the biometric certificate in a memory;

transmitting an electronic transaction over a network, the electronic transaction including transaction biometric data, transaction first data, and a digital signature

generated therefrom, the step of transmitting including the steps of:

receiving a current set of physical characteristics of the user;

generating the transaction biometric data from the current set related to the physical condition of the user;

generating a first hash value signal from the transaction first data and the transaction biometric data;

generating the digital signature from the hash value and a private key signal of the user; and

transmitting the digital signature over the network; and

transmitting the transaction biometric data and the transaction first data over the network; and

authenticating the electronic transaction, including the steps of:

receiving the digital signature, the transaction biometric data and the transaction first data from the network;

retrieving user identification (ID) data from the transaction first data;

retrieving a biometric certificate corresponding to user ID data from a memory;

extracting registration biometric data and the user public key from the biometric certificate;

decrypting the digital signature using the user public key to retrieve the first hash value from the digital signature;

generating a second hash value from the transaction biometric data and the transaction first data;

comparing the first hash value to the second hash value using a first classier;

generating a first validation signal to authenticate the transmission of the transaction first data and the transaction biometric data;

comparing the registration biometric data and

the transaction biometric data using second classifier; and

generating a second validation signal to authenticate the user.

17. The method of claim 16, wherein the step of authenticating further comprises the steps of:

ANDing the first and second validation signals.

18. The method of claim 15, wherein the step of receiving a set of physical characteristics of the user includes the step of:

receiving visual characteristics of the user using a visual reader as the registration biometric input device.

19. The method of claim 15, wherein the step of receiving a set of physical characteristics of the user includes the step of:

receiving speech characteristics of the user using a speech digitizer as the registration biometric input device.

20. The method of claim 15, wherein the step of generating the registration biometric data includes the step of generating a bit sequence greater than about 500 bytes in length as the registration biometric data.

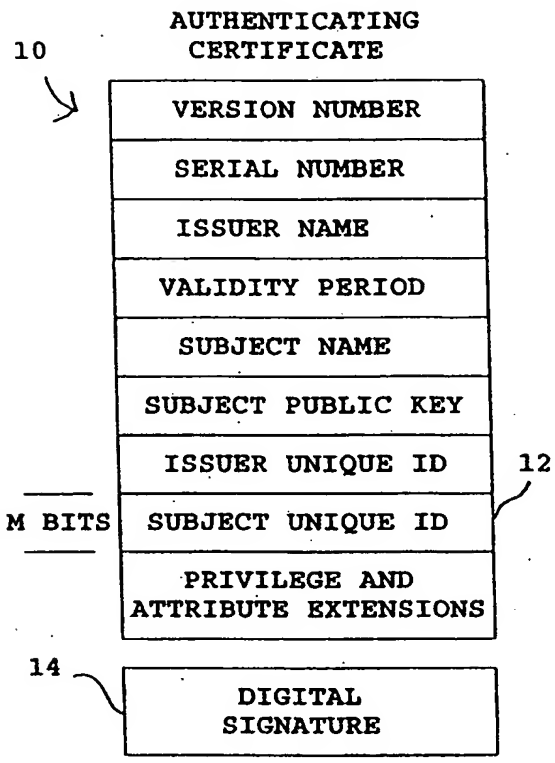


FIG. 1
(PRIOR ART)

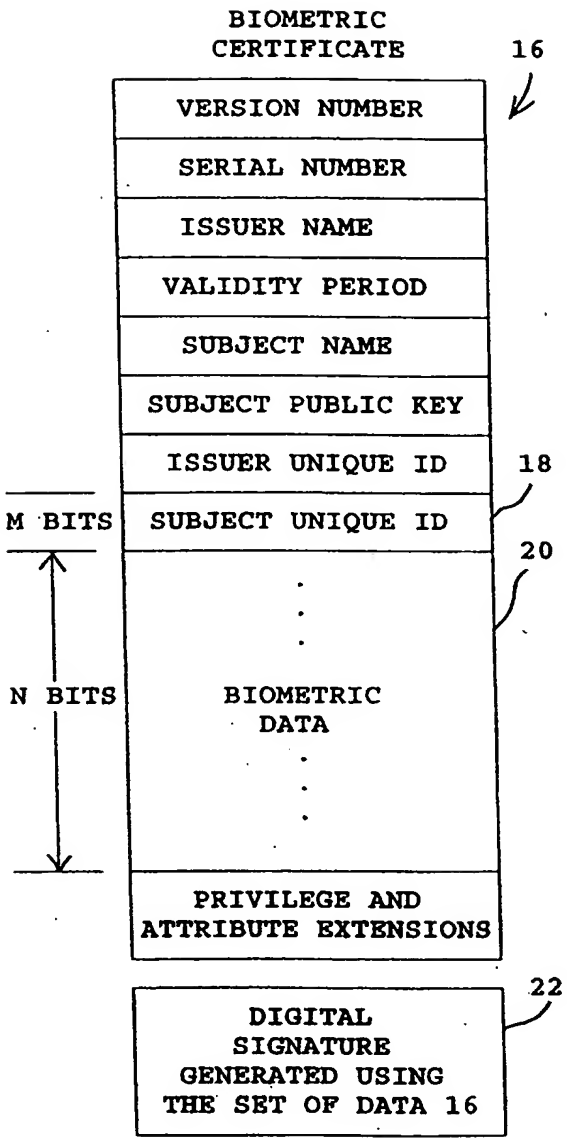


FIG. 2

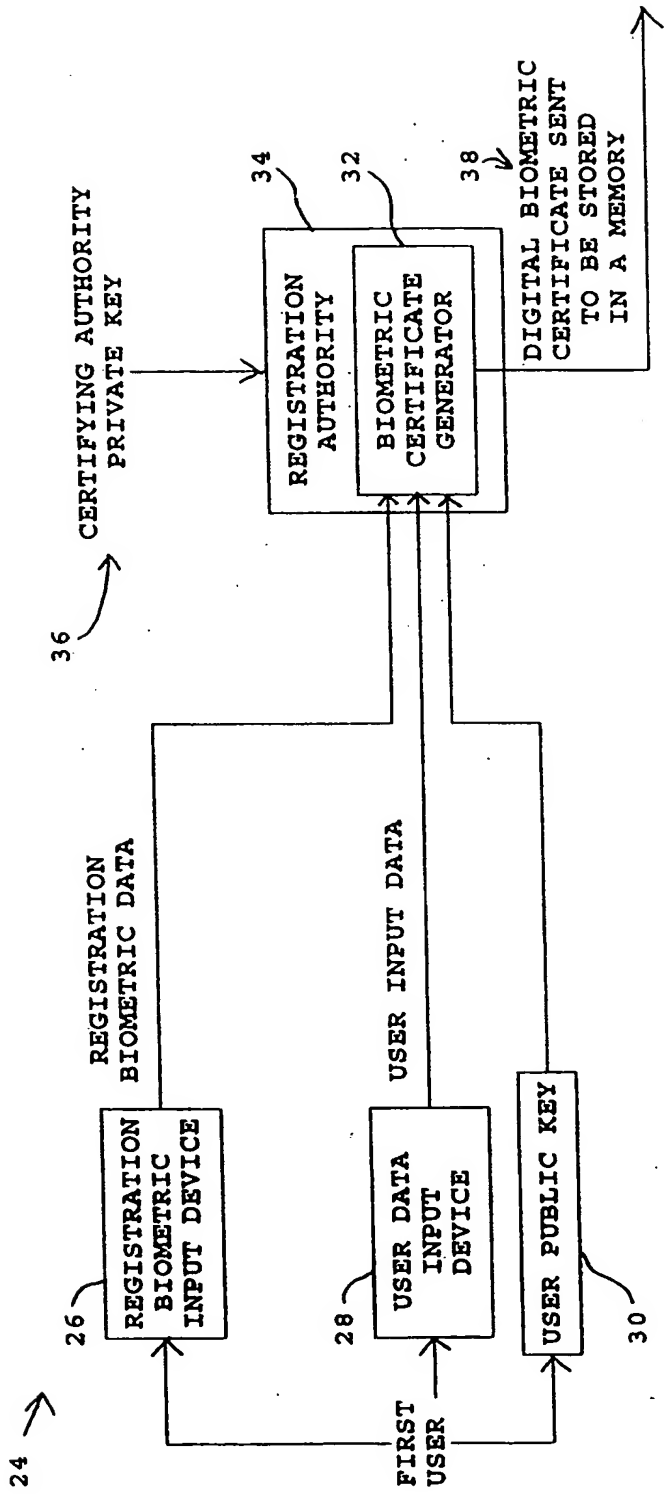

CERTIFYING AUTHORITY PRIVATE KEY
36
REGISTRATION AUTHORITY
34
BIOMETRIC CERTIFICATE GENERATOR
32
38
DIGITAL BIOMETRIC CERTIFICATE SENT TO BE STORED IN A MEMORY
REGISTRATION BIOMETRIC DATA
USER INPUT DATA
REGISTRATION BIOMETRIC INPUT DEVICE
26
USER DATA INPUT DEVICE
28
USER PUBLIC KEY
30
FIRST USER
24

FIG. 3

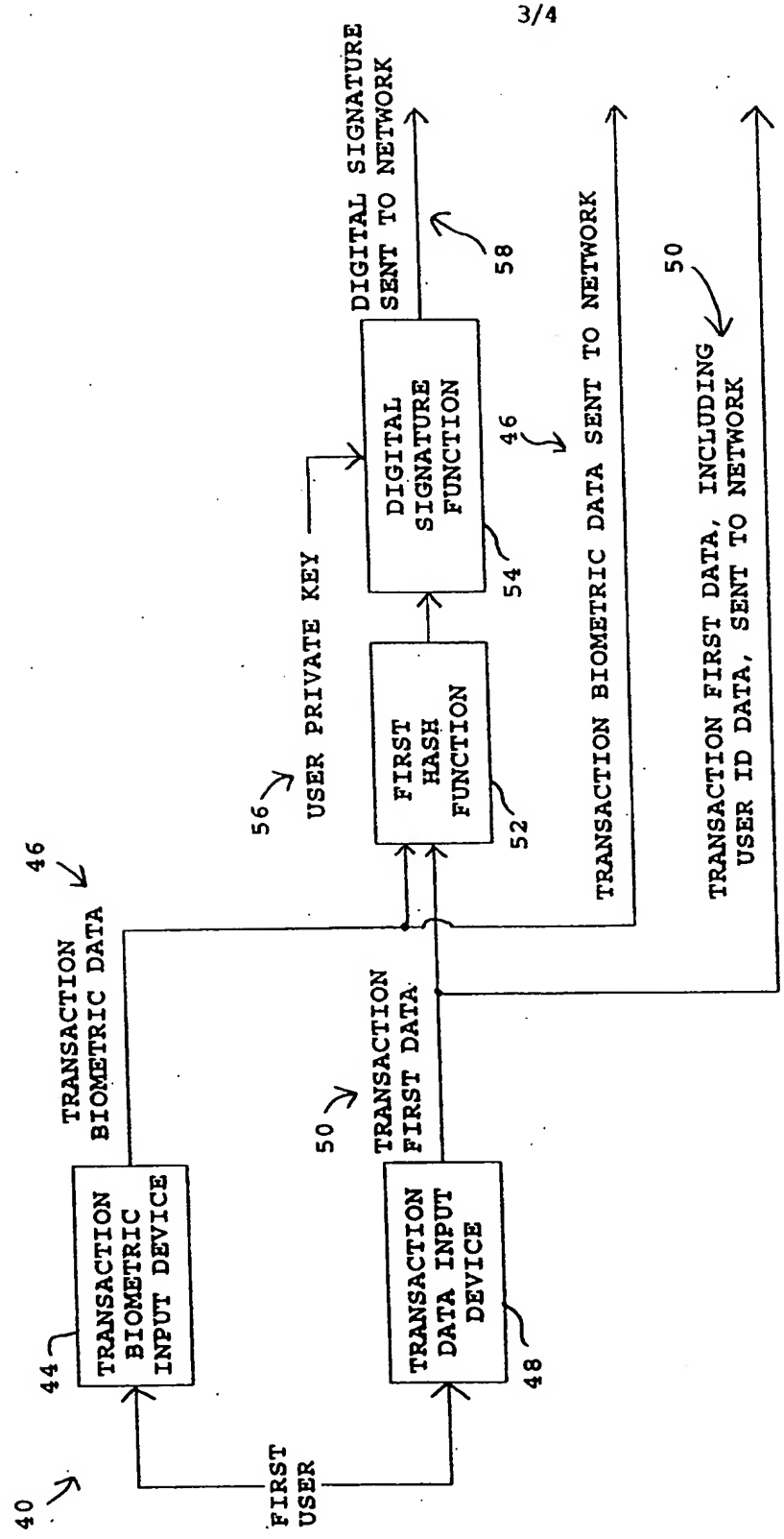

40
FIRST USER
44
TRANSACTION BIOMETRIC INPUT DEVICE
48
TRANSACTION DATA INPUT DEVICE
46
TRANSACTION BIOMETRIC DATA
50
TRANSACTION FIRST DATA
56
USER PRIVATE KEY
52
FIRST HASH FUNCTION
54
DIGITAL SIGNATURE FUNCTION
46
58
DIGITAL SIGNATURE SENT TO NETWORK
TRANSACTION BIOMETRIC DATA SENT TO NETWORK
50
TRANSACTION FIRST DATA, INCLUDING USER ID DATA, SENT TO NETWORK

FIG. 4

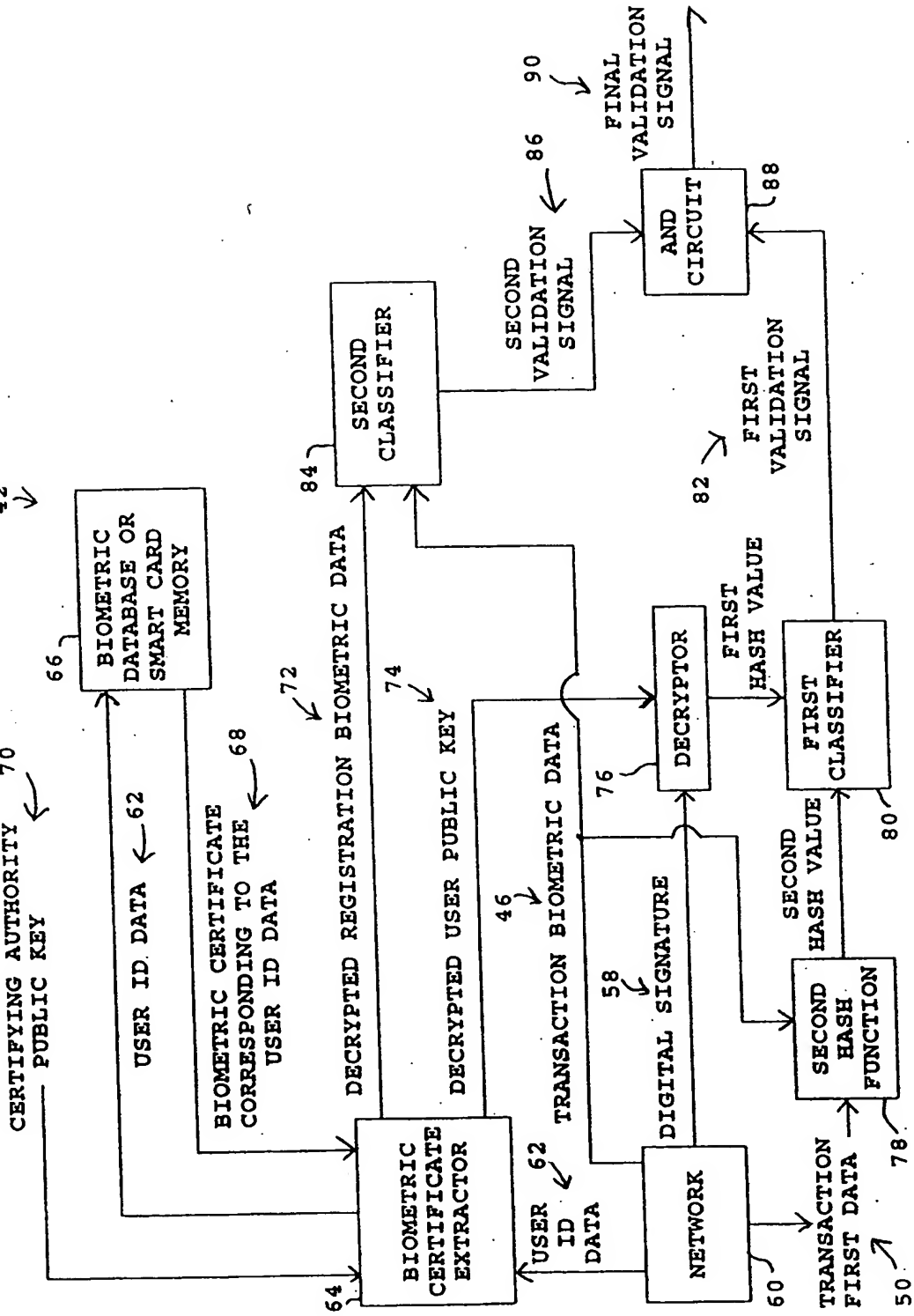

BIOMETRIC DATABASE OR SMART CARD MEMORY
42
66
CERTIFYING AUTHORITY PUBLIC KEY
70
USER ID DATA
62
BIOMETRIC CERTIFICATE CORRESPONDING TO THE USER ID DATA
68
DECRYPTED REGISTRATION BIOMETRIC DATA
72
DECRYPTED USER PUBLIC KEY
74
BIOMETRIC CERTIFICATE EXTRACTOR
64
USER ID DATA
62
TRANSACTION BIOMETRIC DATA
46
DIGITAL SIGNATURE
58
NETWORK
60
TRANSACTION FIRST DATA
50
SECOND HASH FUNCTION
78
SECOND HASH VALUE
80
DECRYPTOR
76
FIRST HASH VALUE
FIRST CLASSIFIER
82
FIRST VALIDATION SIGNAL
SECOND CLASSIFIER
84
SECOND VALIDATION SIGNAL
86
AND CIRCUIT
88
FINAL VALIDATION SIGNAL
90

FIG. 5

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 9/20, H04K 1/00, H04L 9/28, 9/00 — A3

(11) International Publication Number: WO 98/50875

(43) International Publication Date: 12 November 1998 (12.11.98)

(21) International Application Number: PCT/US98/09770

(22) International Filing Date: 8 May 1998 (08.05.98)

(30) Priority Data:
60/046,012 9 May 1997 (09.05.97) US

(71) Applicants: GTE GOVERNMENT SYSTEMS CORPORATION [US/US]; 1209 Orange Street, Wilmington, DE 19801 (US). GTE SERVICE CORPORATION [US/US]; 1209 Orange Street, Wilmington, DE 19801 (US).

(72) Inventors: DULUDE, Robert; 14 Lafayette Circle, Wellesley, MA 02181 (US). MUSGRAVE, Clyde; 3620 Fairfield Place, Frisco, TX 75035 (US).

(74) Agents: SUCHYTA, Leonard, Charles et al.; GTE Service Corporation, 600 Hidden Ridge HQE03G05, Irving, TX 75038 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

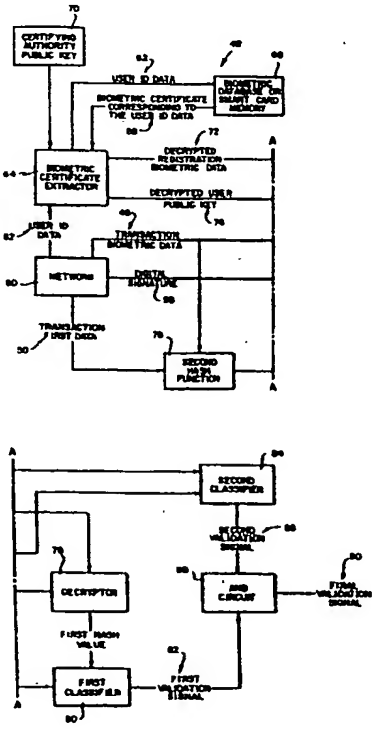
Published
With international search report.

(88) Date of publication of the international search report:
11 February 1999 (11.02.99)

(54) Title: BIOMETRIC CERTIFICATES

(57) Abstract

A biometric certification system includes a biometric certificates extractor system (64) for extracting biometric certificates (68) which may be used for authentication in any electronic transaction having biometric database (66) for pre-storing the obtained biometric data corresponding to physical characteristics of registered users throughout a biometric input device. Subsequent transaction to be conducted over the network (60) have digital signatures (58) generated from the physical characteristics of a current user and from the electronic transaction. The electronic transaction is authenticated by comparing the hash values in the digital signature with re-created hash values. The user is authenticated by comparison against the pre-stored biometric certificates of the physical characteristics of the users in the biometric database.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/09770

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06K 9/20; H04K 1/00; H04L 9/28, 9/00

US CL :Please See Extra Sheet.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 382/115, 116-118, 124, 155, 190; 395/21; 380/2, 9, 23-25, 28, 46; 178/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS: BIOMETRIC, FINGERPRINT, IRIS, EYE, SPEECHM, VOICE, HASH, ENCRYPT, DECRYPT, NEURAL, EXTRACT, CLASS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,868,877 A (FISCHER) 19 SEPTEMBER 1989, see Abstract, col. 10, and figs. 1-4	1, 7, 16
Y	US 4,405,829 A (RIVEST et al.) 20 SEPTEMBER 1983, see Abtract, col. 1-6, and fig. 7	1, 7, 16
Y	US 5,623,545 A (CHILDS et al.) 22 APRIL 1997 see Abstract, col. 1-6, and figs. 1-11	1, 7, 16
Y	US 4,641,349 A (FLOM et al.) 03 FEBRUARY 1987, see Abstract, col. 1-13, and figs. 2-7	1-20
Y	US 5,263,097 A (KATZ et al.) 16 NOVEMBER 1993, see Abstract, col. 1-9, and fig. 3-7	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 25 SEPTEMBER 1998	Date of mailing of the international search report 29 OCT 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JOSE L. COUSO Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/09770

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

382/115, 116-118, 124, 155, 190.; 395/21; 380/2, 9, 23-25, 28, 46; 178/22